

Jiahui Lu

☎ (+1) 404-429-2362 | ✉ jlu355@gatech.edu | 🏠 alanwap.github.io | 📱 AlanWaP | 📺 AlanWaP

Education

Georgia Institute of Technology (Georgia Tech)

Atlanta, Georgia, US

MS IN COMPUTER SCIENCE

Aug 2017 - Dec 2021

- Institute for Information Security & Privacy, College of Computing
- G.P.A. 3.84/4.0

Shanghai Jiao Tong University (SJTU)

Shanghai, China

BSE IN COMPUTER SCIENCE

Sept 2013 - July 2017

- ACM Honored Program, Zhiyuan College
- G.P.A. 3.77/4.3

Work Experience

JD.com Silicon Valley R&D Center

Mountain View, California, US

(Remote in Atlanta, GA, US)

RESEARCH SCIENTIST & ARCHITECT

Feb 2022 -

- Developing secure neural network system with multi-party computation (MPC) frameworks (ABY, Falcon, etc.)
- Exploring scenarios of fully homomorphic encryption in private computing services, e.g. generating multiplication triples

JD.com Silicon Valley R&D Center

Mountain View, California, US

(Remote in Atlanta, GA, US)

RESEARCH INTERN

May 2021 - Aug 2021

- Implemented a protocol to generate distributed RSA secret key pair securely between two servers using oblivious transfer

Research Experience

Institute for Information Security & Privacy, Georgia Tech

Atlanta, Georgia, US

GRADUATE RESEARCH ASSISTANT

Aug 2017 - Dec 2021

- Advisor: Prof. Alexandra Boldyreva & Prof. Vlad Kolesnikov
- Designed secure review protocols supporting instant authorization and user anonymity
- Optimized a zero knowledge proof scheme using MPC-in-the-head to satisfy efficient boolean and arithmetic operations

Security & Privacy group, Cornell Tech

New York City, New York, US

RESEARCH INTERN

Aug 2016 - Dec 2016

- Advisor: Prof. Tom Ristenpart
- Explored side-channel attacks in full text search systems
- Analyzed the security of symmetric encryption schemes as cryptographic commitments

Cornell University

Ithaca, New York, US

EXCHANGE STUDENT

Jul. 2012 - Jun. 2013

- Advisor: Prof. John E. Hopcroft
- Explored the role of units in different convolutional layers of a deep learning network

Lab of Cryptology and Computer Security, SJTU

Shanghai, China

UNDERGRAD RESEARCH ASSISTANT

Jun 2015 - Jun 2016

- Advisor: Prof. Yu Yu
- Explored problems related to Learning Parity with Noise and Fully-Homomorphic Encryption

Publication

Efficient Generic Arithmetic for KKW - Practical Linear MPC-in-the-Head NIZK on Commodity Hardware without Trusted Setup

INTERNATIONAL SYMPOSIUM ON CYBER SECURITY CRYPTOLOGY AND MACHINE LEARNING - CSCML 2021

- Authors: David Heath, Vladimir Kolesnikov, Jiahui Lu
- Conference Talk

Message Franking via Committing Authenticated Encryption

ADVANCES IN CRYPTOLOGY - CRYPTO 2017

- Authors: Paul Grubbs, Jiahui Lu, and Thomas Ristenpart

Side-Channel Attacks on Shared Search Indexes

IEEE SYMPOSIUM ON SECURITY AND PRIVACY - OAKLAND 2017

- Authors: Liang Wang, Paul Grubbs, Jiahui Lu, Vincent Bindschaedler, David Cash, Thomas Ristenpart

Anonymous Review Systems for (Un)linkable Settings

IN PROGRESS

- Authors: Alexandra Boldyreva, Jiahui Lu

Honors & Awards

Qualified to 3rd Round in the 2021 Google Code Jam

INDIVIDUAL

Online

May 2021

4th place in the 2018 ACM-ICPC Southeast USA Regional Contest

TEAM BU SHI MEI GUO REN, GEORGIA TECH

- 1st in Kennesaw State University site

Kennesaw, Georgia, US

Nov 2018

9th place in the 2018 ITA Tech Challenge

INDIVIDUAL

Chicago, Illinois, US

Oct 2018

2nd place in the 2018 Mercer University Spring Programming competition

TEAM YELLOW JACKETS, GEORGIA TECH

- 1st in Division II

Macon, Georgia, US

Feb 2018

Extracurricular Activities

ACM programming team, Georgia Tech

COACH

- Team meeting lecturer
- College team representative in contests. Participated in
 - 2020 Mercer University Spring Programming competition
 - 2020 Southeast USA Regional Contest
 - 2021 ICPC North America Division Championships
 - 2021 ICPC North America Championships

Atlanta, Georgia, US

Aug 2019 - Dec 2021

2020 Mercer University Spring Programming competition

STAFF & PROBLEM WRITER

Macon, Georgia, US

Feb 2020

ISNDES

WEBSITE ADMIN

- Front-end developer of a fan-made forum www.isndes.com

Online

Aug 2018 - Aug 2020

ACM programming team, Georgia Tech

CONTESTANT

Atlanta, Georgia, US

Aug 2017 - Aug 2019